



# CVE-2010-2798

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2010-2798
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-09-08 20:00:00 UTC
<b>Updated</b>	2023-02-13 03:18:00 UTC
<b>Description</b>	The gfs2_dirent_find_space function in fs/gfs2/dir.c in the Linux kernel before 2.6.35 uses an incorrect size value in calculat

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Aura Communication Manager	5.2	All	All	All
Application	Avaya	Aura Communication Manager	5.2	All	All	All
Application	Avaya	Aura Presence Services	6.0	All	All	All
Application	Avaya	Aura Presence Services	6.1	All	All	All
Application	Avaya	Aura Presence Services	6.1.1	All	All	All
Application	Avaya	Aura Presence Services	6.0	All	All	All
Application	Avaya	Aura Presence Services	6.1	All	All	All
Application	Avaya	Aura Presence Services	6.1.1	All	All	All
Application	Avaya	Aura Session Manager	1.1	All	All	All
Application	Avaya	Aura Session Manager	5.2	All	All	All
Application	Avaya	Aura Session Manager	6.0	All	All	All
Application	Avaya	Aura Session Manager	1.1	All	All	All
Application	Avaya	Aura Session Manager	5.2	All	All	All
Application	Avaya	Aura Session Manager	6.0	All	All	All
Application	Avaya	Aura System Manager	5.2	All	All	All
Application	Avaya	Aura System Manager	6.0	All	All	All
Application	Avaya	Aura System Manager	6.1	All	All	All

Application	Avaya	Aura System Manager	6.1.1	All	All	All
Application	Avaya	Aura System Manager	5.2	All	All	All
Application	Avaya	Aura System Manager	6.0	All	All	All
Application	Avaya	Aura System Manager	6.1	All	All	All
Application	Avaya	Aura System Manager	6.1.1	All	All	All
Application	Avaya	Aura System Platform	1.1	All	All	All
Application	Avaya	Aura System Platform	6.0	-	All	All
Application	Avaya	Aura System Platform	6.0	sp1	All	All
Application	Avaya	Aura System Platform	1.1	All	All	All
Application	Avaya	Aura System Platform	6.0	-	All	All
Application	Avaya	Aura System Platform	6.0	sp1	All	All
Application	Avaya	Iq	5.0	All	All	All
Application	Avaya	Iq	5.1	All	All	All
Application	Avaya	Iq	5.0	All	All	All
Application	Avaya	Iq	5.1	All	All	All
Application	Avaya	Voice Portal	5.0	All	All	All
Application	Avaya	Voice Portal	5.1	-	All	All
Application	Avaya	Voice Portal	5.1	sp1	All	All
Application	Avaya	Voice Portal	5.0	All	All	All
Application	Avaya	Voice Portal	5.1	-	All	All
Application	Avaya	Voice Portal	5.1	sp1	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	-	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	-	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	-	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	-	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	-	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	-	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.1	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.1	All	All	All

## References

Reference	Source
<a href="https://access.redhat.com">access.redhat.com</a>   CVE-2010-2798	MISC
Bug 620300 – CVE-2010-2798 kernel: gfs2: rename causes kernel panic	CONF
Support	REDH
404: File not found	CONF
Red Hat Customer Portal	MISC
oss-security - CVE request: kernel: gfs2: rename cases kernel panic	MLIST
SecurityFocus	BUGTI
Linux Kernel GFS2 Directory Rename NULL Pointer Dereference Local Denial of Service Vulnerability	BID
USN-1000-1: Linux kernel vulnerabilities   Ubuntu	UBUN
Red Hat Customer Portal	MISC
<a href="https://kernel/git/torvalds/linux.git">kernel/git/torvalds/linux.git</a> - Linux kernel source tree	MISC
Support / Security / Advisories // MDVSA-2010:198   Mandriva	MAND
oss-security - Re: CVE request: kernel: gfs2: rename cases kernel panic	MLIST

[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE
Support	REDH.
ASA-2010-291 (RHSAs-2010-0723)	CONF
SecurityTracker.com Archives - Linux Kernel GFS2 Rename Null Pointer Dereference May Let Local Users Gain Elevated Privileges	SECTF
VMSA-2011-0012.2	CONF
Support	REDH.
About Secunia Research   Flexera	SECU
kernel/git/torvalds/linux.git - Linux kernel source tree	CONF
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE
Debian -- Security Information -- DSA-2094-1 linux-2.6	DEBI
Red Hat Customer Portal	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**